New MDS Self-Dual Codes over Large Finite Fields

Kenza Guenda [*]

8 avril 2010

Résumé

Nous avons construit des codes MDS qui sont auto-duaux au sens Euclidiens et Hermitiens sur de grands corps finis. Nos codes sont dérivés des codes duadiques cycliques et négacycliques.

Abstract

We construct MDS Euclidean and Hermitian self-dual codes over large finite fields of odd and even characteristics. Our codes arise from cyclic and negacyclic duadic codes.

[*] Faculty of Mathematics USTHB, University of Sciences and Technology of Algiers, B.P 32 El Alia, Bab Ezzouar, Algiers, Algeria

1 Introduction

Let q be a prime power, $\mathbb{F}_q$ a finite field with q elements. An $[n,k]$ linear code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. A linear code of $\mathbb{F}_q^n$ is said to be constacyclic if it is an ideal of the quotient ring $R_n = \frac{\mathbb{F}_q[x]}{x^n-a}$. When $a=1$ the code is called cyclic and when $a=-1$ the codes is called negacyclic. For $\mathsf{x} \in C$, the Hamming weight $wt(\mathsf{x})$ is the number of non zeros coordinates in $wt(\mathsf{x})$. The minimum distance d of C is defined as $d = \min\{wt(\mathsf{x}) : 0 \neq \mathsf{x} \in C\}$. If the parameters of the code C verify $n-k+1=d$, then the code is said to be maximum distance separable (MDS). The minimum distance of a code is related to its capacity of correctability. For that the MDS codes are optimum in this sense. Furthermore, the MDS codes find application in algebraic geometry [6]. They are also related to geometric objects called n-arcs and to combinatorial objects called orthogonal arrays [19, Ch. 11].

The Euclidean dual code $C^{\perp}$ of the code C is defined as $C^{\perp} = \{\mathsf{x} \in \mathbb{F}_q^n : \sum_{i=1}^{n} x_i y_i = 0\,, \forall \mathsf{y} \in C\}$. If $q=p^2$ the Hermitian dual code $C^{\perp h}$ of C is defined as $C^{\perp h} = \{\mathsf{x} \in \mathbb{F}_q^n : \sum_{i=1}^{n} x_i y_i^p = 0\,, \forall \mathsf{y} \in C\}$. A code is called Euclidean self-dual or Hermitian self-dual if it satisfies $C = C^{\perp}$ or $C = C^{\perp h}$. For $q \equiv 1 \mod 4$ a self-dual code over $\mathbb{F}_q$ exists if and only if n is even, and for $q \equiv 3 \mod 4$ a self-dual code over $\mathbb{F}_q$ exists if and only if $n \equiv 0 \mod 4$ [19, Ch. 19]. The linear codes which are close to the Gilbert-Varshamov bound are good and interesting for practical uses. It turns out that the self-dual codes codes satisfies a modified Gilbert-Varshamov-bound [21]. This makes this family of codes a very attractable family.

This paper is devoted to the construction of MDS Euclidean and Hermitian self-dual codes from cyclic duadic codes and negacyclic duadic codes. Our results, also can be seen as construction of MDS self-dual codes over large fields. This subject is at the heart of many recent research papers [4, 10, 16]. Whereas, all these constructions care about the computational complexity, our does not. For that, we reach optimum parameters.

Recently, Gulliver et al. [9] constructed MDS self-dual codes of length q over $\mathbb{F}_q$ from extended Reed-Solomon codes, whenever $q = 2^m$. It turns out, that these codes are extended duadic codes. For q odd the construction of [9] is impossible [19] p. 598. Our construction is more general for fields of odd or even characteristics, and allows us to construct MDS Euclidean and Hermitian self-dual codes from the cyclic duadic codes with various lengths. Blackford [3] studied the negacyclic codes over finite fields by using the multipliers. He gave conditions on the existence of Euclidean self-dual codes. We generalize his work to the Hermitian case. We give necessary and sufficient conditions on the existence of Hermitian self-dual codes from the negacyclic codes. Hence, by using our previous results, the decomposition of the polynomial $x^n + 1$ and the results of Blackford we construct new MDS Euclidean and Hermitian self-dual codes from the negacyclic duadic codes. Furthermore, we give conditions on the existence of Euclidean self-dual codes which are extended negacylic.

The paper is organized as follows : In Section 2 we construct MDS self-dual codes (Euclidean and Hermitian) from cyclic duadic codes. First we give cyclic MDS codes over $\mathbb{F}_q$, when n divides $q-1$ and n divides q^2+1. Furthermore, by using a result from [8] on the existence of the μ_{-q} splitting we give extended duadic codes which are new MDS Euclidean or Hermitian self-dual codes.

In Section 3 we generalize the work of [3] to the Hermitian cases. We give necessary and sufficient condition on the existence of negacylic Hermitian self-dual codes. We construct negacylic MDS self-dual codes for both the Euclidean and the Hermitian cases.

Several examples have been given from of our results paper. Some of them reach the best known bounds or even exceed the one given by Kim and Lee [15, Table 1] or the ones in [4,10,16]. We close by giving a table of MDS self-dual codes of length 18 over prime fields.

2 Duadic MDS Self-Dual Codes

Assmus and Mattson [1] have shown that every cyclic code of prime length t over $\mathbb{F}_{p^i}$ is MDS for all i, except a finite number of primes p. For cyclic codes of composite length, Pedersen and Dahl [20] proved that when n divides $q = p^h$, there is no-trivial MDS cyclic code over $\mathbb{F}_{p^h}$ if and only if $h = 1$. In this case any cyclic code is MDS and with generator polynomial $g(x) = (x-1)^{p-k}$. For the previous reasons we consider only the case $(n, q) = 1$ and q a prime power. The integer n can be prime or composite and we propose the following Lemma.

Lemma 1 *Let q be a prime power. Then if n divides $q-1$, the polynomial $g_j(x) = \prod_{i=j}^{n-k+j-1}(x-\alpha^i)$ generate generate an MDS code.*

Proof. If n divides $q-1$ i.e., ord $_n(q) = 1$, then each cyclotomic class modulo n contains exactly one element. For a fixed $k > 0$, and α an n^{th} root of unity the polynomial $g_j(x) = \prod_{i=j}^{n-k+j-1}(x-\alpha^i)$ generate an MDS cyclic code, and that because g has $n-k$ consecutive roots, by the BCH bound the minimum distance d is such that $d \geq n-k+1$, and then we have the equality by the Singleton bound. ■

2.1 Euclidean Self-dual MDS Codes over $\mathbb{F}_q$

This section shows that there exists MDS Euclidean self-dual codes over $\mathbb{F}_q$ and which arise from cyclic duadic codes.

The following Lemma is useful for the next.

Lemma 2 *([5,14, Proposition 4.7,Theorem 4.4.9]), Let C be an $[n,k]$ cyclic code over $\mathbb{F}_q$ with defining set $T \subset Z_n = \{0,1,\ldots,n-1\}$. Then the following holds :*

(i) The Euclidean dual $C^{\perp}$ is also cyclic and has defining set $Z_n \setminus (-1)T$.

(ii) The Hermitian dual $C^{\perp h}$ is also cyclic and has defining set $Z_n \setminus (-q)T$.

When we consider an odd integer n which divides $q-1$, hence q is a residue quadratic modulo n,(denoted by $q = \square \mod n$). Then from [23, Theorem

1], there exists a duadic code of length n. Now we will construct some of these duadic codes. Consider the following cyclic code D_1 with defining set $T_1 = \{1, 2, \ldots, \frac{(n-1)}{2}\}$. By Lemma 1, the code D_1 is an $[n, \frac{(n+1)}{2}, \frac{(n+1)}{2}]$, MDS code over $\mathbb{F}_q$, by Lemma 2 its dual $C_1 = D_1^{\perp}$ is also cyclic with defining set $T_1 \cup \{0\}$. The code C_1 is self-orthogonal as $T_1 \subset T_1 \cup \{0\}$ and is with dimension $\frac{n-1}{2}$ and with minimum distance $\frac{n-1}{2}$, hence also MDS.

This gives that the code C_1 is an even-like duadic code whose splitting is given by μ_{-1} due to the following Lemma.

Lemma 3 *([14, Theorem 6.4.1]) Let C be any $[n, \frac{n-1}{2}]$ cyclic code over $\mathbb{F}_q$, with q a prime power. Then C is self-orthogonal if and only if C is an even like duadic code whose splitting is given by μ_{-1}.*

This gives us a pair of duadic codes $D_1 = C_1^{\perp}$ and $D_2 = C_2^{\perp}$ and a pair of even like duadic code $C_2 = \mu_{-1}(C_1)$. Hence the following result.

Lemma 4 *Let n be an odd integer which divides $q-1$, then there exists a pair of MDS codes D_1, D_2 with parameters $[n, \frac{(n+1)}{2}, \frac{(n+1)}{2}]$, which are duadic codes with the splitting given by μ_{-1}.*

Since n is odd, we want to extend the codes D_i for $1 \leq i \leq 2$ in such a way the extended code is self-dual. This is possible provided the hypothesis of the following Lemma are satisfied.

Lemma 5 *([14, Theorem 6.4.12]) Let D_1 and D_2 be a pair of odd-like duadic* *codes of length n over $\mathbb{F}_q$. Assume that*

$$1 + \gamma^2 n = 0 \tag{1}$$

has a solution in $\mathbb{F}_q$. Then if μ_{-1} gives the splitting from D_1 and D_2, then $\widetilde{D_1}$ and $\widetilde{D_2}$ are self-dual. Here $\widetilde{D_i} = \{\widetilde{\mathsf{c}} \,|\, \mathsf{c} \in D_i\}$ for $1 \le i \le 2$ and $\widetilde{\mathsf{c}} = c_0 \ldots c_n c_\infty$ with $c_\infty = -\gamma \sum_{i=0}^{n-1} c_i$.

In general it is not always possible to find a solution to the equation (1) in $\mathbb{F}_q$. Furthermore, extending an MDS code does not give always an MDS code. But under some conditions this can be possible, as proved by Hill [12]. For $n = q - 1$ we have $\gamma = 1$ is a solution of (1). Moreover, if the code is a Reed-Solomon code, then by a result of Macwilliams and Sloane [19, Theorem.10.3.1] the extended code is also MDS. In the landmark textbook [14] the solution of the equation (1) is discussed, when n is an odd prime number. The following Lemma generalize their results to $n = p^m$.

Lemma 6 *Let $q = r^t$, with r an odd prime, t an odd integer and $n = p^m$ such that n divides $q - 1$. Then there is a solution to the equation (1) in $\mathbb{F}_q$, whenever one of the following holds.*

1. *$r \equiv 3 \mod 4$, $p \equiv 3 \mod 4$ and m odd;*
2. *$r \equiv 1 \mod 4$ and $p \equiv 1$ or $3 \mod 4$;*

Proof. As mentioned before if n divides $q - 1$, then $q = \square \mod p$. This gives that $q = \square \mod r$. Hence if $p \equiv 3 \mod 4$ and $r \equiv 3 \mod 4$, there is a solution γ to the equation $1+\gamma^2 p=0$ [14, Lemma 6.6.17]. If m is odd, hence γ^m is a solution to the equation (1). Now, assume $q \equiv 1 \mod 4$ and $p \equiv 1$ or $3 \mod 4$. The equation $1+\gamma^2 p=0$ [14, Lemma 6.6.17] has a solution in $\mathbb{F}_q$. As for the previous case, if m is odd γ^m is a solution to the equation (1). Now, assume that m is even, since for such p and q there is a solution to $1+\gamma^2 p=0$ in $\mathbb{F}_q$ [14, Lemma 6.6.17]. This gives $(\gamma^m)^2=\frac{1}{p^m}$. But, since $r \equiv 1 \mod 4$, then -1 is a quadratic residue in $\mathbb{F}_r \subset \mathbb{F}_q$ [14, Lemma 6.2.4]. Then, there exists an $a \in \mathbb{F}_q$, such that $a^2=-1$. Hence $a\gamma^m$ is a solution of the equation (1) in $\mathbb{F}_q$. ■

In the following result we give Euclidean self-dual codes which are MDS.

Theorem 7 *Let $q=r^t$ be a prime power (even or odd), n an odd divisor of $q-1$. Then there exists a pair of D_1, D_2 of MDS odd-like duadic codes, with splitting μ_{-1} and where the even-like duadic codes are MDS self-orthogonal and $T_1=\{1,\ldots,\frac{n-1}{2}\}$. Furthermore, the following holds :*

(i) If $q=2^t$, with t odd and $n=p$ an odd prime, then the extended codes $\widetilde{D_i}$ are $[n+1,\frac{n+1}{2},\frac{n+3}{2}]$ MDS and Euclidean self-dual codes.

(ii) If $q=r^t$, with t even and n odd and divides $r-1$, then the extended codes $\widetilde{D_i}$ for $1 \leq i \leq 2$ are $[n+1,\frac{n+1}{2},\frac{n+3}{2}]$ MDS Euclidean self-dual codes.

(iii) If $q=r^t$, with $r \equiv 3 \mod 4$, t odd and $n=p^m$, with p a prime such that $p \equiv 3 \mod 4$ and m is odd, then the extended codes $\widetilde{D_i}$ are $[n+1,\frac{n+1}{2},\frac{n+3}{2}]$ MDS and Euclidean self-dual codes.

(iv) If $q=r^t$, with t odd, p a prime such that $r \equiv p \equiv 1 \mod 4$ and

$n = p^m$, then the extended codes $\widetilde{D_i}$ are $[n+1, \frac{n+1}{2}, \frac{n+3}{2}]$ MDS and Euclidean self-dual codes.

Proof. Lemma 4 gives a pair D_1, D_2 of MDS odd-like duadic codes, with splitting μ_{-1} and where the even-like duadic codes are MDS self-orthogonal and $T_1 = \{1, \ldots, \frac{n-1}{2}\}$. If $q = 2^t$, t odd and $n = p$ an odd prime which divides $q - 1$, hence $q = \square \mod n$. From [14, Lemma 6.6.17], there is a solution to the equation (1) in $\mathbb{F}_q$. Hence from Lemma 5, the extended codes $\widetilde{D_i}$ are self-dual. If t is even and n is an odd integer which divides $r-1$, from [14] p. 227 there is a solution of the equation (1) in $\mathbb{F}_{r^2} \subset \mathbb{F}_q$, since the coefficients are in $\mathbb{F}_r$. Further, if we assume $r \equiv 3 \mod 4$, t odd and $n = p^m$ with m odd and such that $p \equiv 3 \mod 4$, by Lemma 6, there is a solution to the equation (1). Hence from Lemma 5 the extended codes $\widetilde{D_i}$ are self-dual. Similarly if we assume $r \equiv 1 \mod 4$, t odd and $n = p^m$ such that $p \equiv 1$ or $3 \mod 4$, we have a solution to the equation (1) by Lemma 6. Hence from Lemma 5 the extended codes $\widetilde{D_i}$ are self-dual. Now we prove that $\widetilde{D_i}$ are MDS. Let c be a codeword of D_i of weight $\frac{n+1}{2}$, the minimum weight of $\widetilde{D_i}$ is increasing by 1 provided

$$-\gamma \mathsf{c}(1) = -\gamma \sum_{i=0}^{n-1} c_i = c_\infty \neq 0. \tag{2}$$

But $\gamma \neq 0$, hence to have (2) it suffices to verify that $\mathsf{c}(1) \neq 0$. Since $c(x) = a(x)g(x)$ for some $a(x) \mod (x^n - 1)$ and $g(x) = \prod_{i=1}^{\frac{n-1}{2}} (x - \alpha^i)$. $g(1) \neq 0$, also $a(1) \neq 0$ otherwise, $a(x)$ is a multiple of $(x-1)g(x)$. Hence by the BCH bound the weight is $\geq 1 + \frac{n+1}{2}$, by the singleton bound we get the equality.

n	q	n	q
4	7,13,19,31,43,49,79,97,11^2,13^2,17^2,31^2	6	17,9^2,11^2,31^2
8	8,29,43,71,13^2,2^9	10	19,37,73,109,19^2
12	23,67,89	14	53^2
16	31^2	18	103^2
24	2^{11}	30	59^2
32	32,5^3	74	293,2^9
84	167	90	2^{11}

Table 1 – Euclidean Self-dual MDS Codes over $\mathbb{F}_q$ obtained by Theorem 7

■

2.2 Hermitian Self-Dual MDS Codes

Let q be a power of an odd prime r. In this part we will construct MDS self-dual codes over $\mathbb{F}_{q^2}$ of length $n+1$, with $n|q^2+1$.

First remark that, when n divides q^2+1, then the multiplicative order of q^2 modulo n is equal to 2. This implies that all the cyclotomic classes $C(i)$ modulo n are reversible with cardinality 1 or 2, that is because $|C(i)|$ divides $\operatorname{ord}_n q^2$. It follows that, if n is odd then $C(i)=\{i,-i\}$ for any $i\neq 0$. If we consider the cyclic code generated by the polynomial

$$g_s(x)=\prod_{i=\frac{n-1}{2}-s}^{i=\frac{n-1}{2}+s+1}(x-\alpha^i) \text{ with } 0\leq s\leq \frac{n-1}{2},$$

it is an $[n,n-2s-2,2s+3]$ MDS cyclic code. The polynomial $g_s(x)$ has

$2s+2$ consecutive roots

$$\alpha^{\frac{n-1}{2}-s}, \alpha^{\frac{n-1}{2}-s+1}, \ldots, \alpha^{\frac{n-1}{2}+1}, \ldots, \alpha^{\frac{n-1}{2}+s+1}.$$

This gives a cyclic MDS code with odd dimension $k = n - 2s - 2$.

Now, consider $n = p^m$ such that n divides q^2+1 and $p^m \equiv 1 \mod 4$, for $s = \frac{n-1}{4} - 1$, the polynomial g_s generate a cyclic MDS code D_1 of parameter $[n, \frac{n+1}{2}, \frac{n+1}{2}]$. Lemma 2 gives that Hermitian dual of D_1 is with defining set $Z_n \setminus (-qT)$. Since $\operatorname{ord}_n q^2$ is even (equal to 2), then the multiplier μ_{-q} gives a splitting [7, Proposition 13]. Hence the code D_1 is one of the odd-like duadic codes and then $D_1^{\perp h} = C_1$ is the even like duadic with defining set $T \cup \{0\}$. Hence $C_i \subset C_i^{\perp h} = D_i$. As for the Euclidian case, using the usual extension of an orthogonal code does not give always a self-dual code. If we consider in $\mathbb{F}_{q^2}$ the equation

$$1 + \gamma^{q+1} n = 0, \tag{3}$$

it has always a solution in $\mathbb{F}_{q^2}$ if we assume $n \in \mathbb{F}_r$ as mentioned in [5]. For $1 \leq i \leq 2$, the extended codes are $\widetilde{D_i} = \{\widetilde{\mathsf{c}} \,|\, \mathsf{c} \in D_i\}$, with $\widetilde{\mathsf{c}} = c_0 \ldots c_n c_\infty$, $c_\infty = -\gamma \sum_{i=0}^{n-1} c_i$ and γ is solution of the equation (3).

Since in this case the splitting is given by μ_{-q}, the codes $\widetilde{D_i}$ are Hermitian self-dual [5, Proposition 4.8]. By a similar argument as in Theorem 7, the extended codes are also MDS, since the codes D_i are MDS. This prove the following Theorem.

Theorem 8 *Let $q = r^t$ be a prime power, $n = p^m \in \mathbb{F}_r$ a divisor of q^2+1,*

n	q	n	q
6	3,7,13,17,23,37,43,47,53,63,67,73,83	14	31,47,73,83
18	13	30	17
38	31	42	73
54	23,83	62	11
138	37	182	19
234	89	422	29

TABLE 2 – Hermitian Self-dual MDS Codes over $\mathbb{F}_{q^2}$ obtained by Theorem 8

where $p^m \equiv 1 \mod 4$. *There exists Hermitian self-dual codes over* $\mathbb{F}_{q^2}$ *which are* MDS *and extended duadic codes with the splitting given* μ_{-q} *and with parameters* $[n+1, \frac{n+1}{2}, \frac{n+3}{2}]$.

3 Negacyclic Duadic Codes

It was proved in [11] that if n is odd, then the negacyclic codes are equivalent to cyclic codes, for that we consider only negacyclic codes with even length.

Now in order to use it latter we review the factorization of the polynomial x^n+1 over $\mathbb{F}_q[x]$. This can be found in [2,17,18]. We also assume $(n,q)=1$, so that the polynomial x^n+1 does not have multiple roots.

The roots of x^n+1 are $\delta, \delta\xi, \ldots, \delta\xi^{n-1}$, where ξ is a primitive nth root of unity and $\delta^n = -1$. Hence $\xi = \delta^2$, δ is a primitive $2n$th root of unity. Hence δ lies in an extension field $\mathbb{F}_{q^s}$, with s equal to the multiplicative order of q modulo $2n$. Let ω be a primitive element of $\mathbb{F}_{q^s}$, hence we can take $\delta = \omega^t$

and $\xi = \omega^{2t}$, with $t = \frac{q^s-1}{2n}$. Then the following holds.

$$x^n + 1 = \prod_{i=0}^{n-1}(x - \delta\xi^i) = \prod_{i=0}^{n-1}(x - \omega^{t(1+2i)}) = \prod_{i=0}^{n-1}(x - \delta^{(1+2i)}).$$

To each irreducible factor of x^n+1 corresponds a cyclotomic class modulo $2n$. δ^{2i+1} and δ^{2j+1} are said to be conjugate if they are roots of a same irreducible factor of $x^n + 1$.

If we denote by O_{2n} the set of odd integers from 1 to $2n - 1$. The defining set of negacyclic code C of length n is the set $T = \{i \in O_{2n} : \delta^i \text{ is a root of } C\}$. It will be the union of q-cyclotomic classes modulo $2n$. The dimension of the negaclic code with defining set T is $n - |T|$. Nuh et al. [2] gave a negacylic BCH bound given. That is if T has $d - 1$ consecutive odd integers, then the minimum distance is at least d.

Lemma 9 *([3, Theorem 2] If C is a negacyclic code with defining set T, then $C^{\perp}$ (the Euclidian dual of C) is a negacyclic code with defining set*

$$T^{\perp} = \{i \in O_{2n} : -i(\mod 2n) \notin T\}$$

Let $s \in \{1, \ldots, 2n - 1\}$ such that $(s, 2n) = 1$, a multiplier of R_n is the map :

$$\begin{aligned} \mu_s : R_n &\longrightarrow \mathbb{F}_q^n \\ a(x) &\longmapsto \mu_s(a(x))(\mod x^n + 1), \end{aligned} \tag{4}$$

μ_s is an automorphism of R_n. If C is an ideal of R_n with defining set T , then $\mu_s(C)$ is an ideal of R_n with defining set $\{i \in O_{2n} \,|\, si \in T\}$. μ_s induces the following map

$$\begin{aligned} \mu'_s : O_{2n} &\longrightarrow O_{2n} \\ i &\longmapsto \mu'_s(i) = si(\mod 2n), \end{aligned} \tag{5}$$

The multiplier $\mu_{2n-1} = \mu_{-1}$ has the effect to replace x by x^{-1}, since $x^{2n} = 1$ in R_n.

Lemma 10 *([3, Theorem 3]) If $N = 2^a n'$ for some odd integer n', then self-dual negacyclic codes over $\mathbb{F}_q$ of length N exist if and only if*

$$q \neq -1(\mod 2^{a+1}).$$

If $a = 1$, then self-dual negacyclic codes over $\mathbb{F}_q$ of length N exist if and only if

$$q \equiv 1 \mod 4.$$

As a Corollary of Lemma 10 the negacyclic code of length $q+1$ and defining set $T = \{i \text{ odd} : 1 \leq i \leq q\}$ is an Euclidean self-dual MDS code over $\mathbb{F}_q$ as proved in [3]. The following results is more general than the ones given in [3] .

Theorem 11 *Let $n = 2n'$ for some odd integer n', q an odd prime power such that $q \equiv 1 \mod 4$, $q + 1 = 2n''$, with $n'|n''$ and n'' odd. Then there exists MDS negacyclic Euclidean self-dual code of parameters* $[n, n/2, n/2+1]$

having defining set

$$T = \{\frac{q+1}{2} + i : -(n'-1) \leq i \ \textit{even} \ \leq (n'-1)\}.$$

Proof. Consider a negacyclic code C with such length n over $\mathbb{F}_q$. Assume $\delta^{2i'+1}$ is a root of C, hence $(\delta^{2i'+1})^{q+1} = \delta^{2i'(q+1)}\delta^{q+1} = \delta^{2jn}\delta^{q+1} = \delta^{q+1}$. Then for an odd $i \in O_{2n}$ the conjugate of δ^i is $\delta^{iq} = \delta^{q+1-i}$. Hence we have $C(i) = \{i, q+1-i\}$. It is clear that for $i \in O_{2n}$ we have $|C(i)| \leq 2$. And $i = q+1-i \mod 2n \iff i = \frac{q+1}{2} + kn$. Hence for i even, such that $1 \leq i \leq (n'-1)$ we have $|C(\frac{q+1}{2}+i)| = |\{\frac{q+1}{2}+i, \frac{q+1}{2}-i\}| = 2$ and for $i = 0$ $|C(\frac{q+1}{2})| = 1$. Now, consider a negacyclic code with the following defining set :

$$T = \cup_{i=0}^{n'-1} C(\frac{q+1}{2}+i) = \{\frac{q+1}{2} + i : -(n'-1) \leq i \text{ even } \leq (n'-1)\}.$$

Assume there exists two differents integers i and j such that $0 \leq i \leq n'-1$, $0 \leq j \leq n'-1$ and $C(\frac{q+1}{2}+i) = C(\frac{q+1}{2}+j)$. Hence $\frac{q+1}{2}+i = \frac{q+1}{2}+j+2kn \iff i-j = 2kn$. That is $i-j$ is a multiple of $2n$. But we have $i-j \leq n$, which is impossible. Furthermore, from Lemma 10 we have $C(i) \neq C(-i) \mod 2n$. If we assume the existence of two different i', j' in T such that $C(i') = C(-j')$, hence there exists i and j such that $i' = \frac{q+1}{2} + i$ and $j' = \frac{q+1}{2} + j$. But, $C(i') = C(-j') \iff \frac{q+1}{2} + i = 2kn - \frac{q+1}{2} - j \iff -(q+1+2k'n) = i+j = n(-\frac{q+1}{n} + 2k)$, this gives that n divides $i+j$, which is impossible since $-(n'-1) \leq i, j \leq (n'-1)$. This implies, that $-T \cap T = \emptyset$ and the

n	q	n	q	n	q
6	5,17,29,53,197	10	9,29,49,13^2	14	13
18	17,53,89,101,197	22	109,197	26	25,181,233
30	29,89,149	34	101,13^2	38	37,113
42	41,293,461	50	49,149,	54	53,269

Table 3 – Euclidean Self-dual MDS Codes over $\mathbb{F}_q$ obtained by Theorem 11

redundancy of the code is equal to n', hence the code is self-dual. The code is MDS, since there is n' successive roots and hence by the BCH bound the minimum distance is at least $n'+1$, hence by the Singleton bound we have equality. ■

Theorem 12 *Let $n = 2^a n'$ for some odd integer n', q an odd prime power such that $q \equiv 1 \mod 2^{a+1}n''$, $n'|n''$ and n'' odd. Then there exists MDS negacyclic Euclidean self-dual code of parameters $[n, n/2, n/2+1]$ having defining set*

$$T = \{i \text{ odd}:\ 1 \leq i \leq n-1\}.$$

Proof. In this case we have $\xi \in \mathbb{F}_q$, hence $\xi^q = \xi$. We will show that the conjugate of $\delta^{2i+1} = \delta\xi^i$ is exactly it self. This means that each cyclotomic class contains only one element. Namely

$$(\delta\xi^i)^q = \delta^q\xi^i = \delta\delta^{q-1}\xi = \delta(\delta^{2n})^{\frac{q-1}{2n}}\xi^i = \delta\xi^i.$$

Now we consider the negacyclic code with defining set $T = \{i \text{ odd}:\ 1 \leq i \leq n-1\}$, by Lemma 10 we obtain $C(i) \neq C(-i)$. Furthermore, for different

n	q	n	q	n	q
6	13,25,37,49,61,73	10	41,61,81	12	49,73,97
14	29,113	18	37,73,109	20	41,81,121
24	49,193	26	53,157	28	169,281,337
30	61,121,181	34	409	36	73,433

TABLE 4 – Euclidean Self-dual MDS Codes over $\mathbb{F}_q$ obtained by Theorem 12

i and j in T we cannot have $C(i) = C(-j)$. Because, if i is the case we will have $2nk - i = j$, since in each class there is only one element. Hence $i + j = 2nk$, which is impossible, because $i \leq n-1$ and $j \leq n-1$. Which implies $-T \cap T = \emptyset$ and $|T| = \frac{n}{2}$. Then from Lemma 9, we obtain $T^{\perp} = T$. Hence the code is self-dual. By the BCH bound the minimum distance is $\frac{n}{2} + 1$ ■

Lemma 13 *Let C be a negacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set T. Then the Hermitian dual is a negacyclic code with defining set*

$$T^{\perp h} = O_{2n} \setminus (-iq)T\}.$$

Proof. Let $\overline{C} = \{(a_0^q, \ldots, a_{n-1}^q) : (a_0, \ldots, a_{n-1}) \in C\}$. By an analogous argument as in [5, Proposition 3.1] one can show that $\overline{C} = \mu_q(C)$. This gives that the code $\overline{C}$ is a negacyclic code with defining set $T_{\overline{C}} = qT = \{iq : i \in T\}$. By noticing that $C^{\perp h} = \overline{C}^{\perp}$, we get that

$$T_{\overline{C}}^{\perp} = \{i \in O_{2n} : -i(\mod 2n) \notin qT\}.$$

Since μ_q is an automorphism on R_n, hence induces a permutation acting on the elements of O_{2n}. Thus we have :

$$-i(\mod 2n) \notin qT \iff -qi \mod 2n \notin q^2T. \tag{6}$$

But over $\mathbb{F}_{q^2}$ all the cyclotomic classes are stable by multiplication by q^2, hence the equation (6) is equivalent to $-qi \mod 2n \notin T$. Then,

$$T^{\perp h} = \{i \in O_{2n} : -iq(\mod 2n) \notin T\} = O_{2n} \setminus (-q)T\}.$$

■

Proposition 14 *If $N = 2^a n'$ for some odd integer n', there exists a Hermitian self-dual code over $\mathbb{F}_{q^2}$ of length N if and only if*

$$q \neq -1 \mod 2^{a+1}. \tag{7}$$

Proof. From Lemma 13, the code C is Hermitian self-dual if and only if we have $T = O_{2n} \setminus (-iqT)$, hence C is Hermtian self-dual if its defining set T satisfies the following

$$2N - iq \notin T \iff i \in T. \tag{8}$$

Then, if there exists an odd $i \in O_{2N}$, such that $C_{q^2}(i) = C_{q^2}(-qi) \mod 2N$, the code C is not self-dual. If a such i exists, then there is an integer m

such that $-iq \equiv q^{2m}i(\mod 2N)$. Hence, $2^{a+1}n'k = (q^{2m-1}+1)qi$ i.e., $2^{a+1}n'|(q^{2m-1}+1)qi$. Since n' is odd we can choose i such that $n' \equiv i$ mod $2N)$. We need only check that $2^{a+1}|(q^{2m-1}+1)q$. Since q is odd hence $2^{a+1}|q^{2m-1}+1$. Thus it is sufficient only to check that $q \equiv -1 \mod 2^{a+1}$. ■

For $a = 1$, the equation (7) becomes $q \equiv 1 \mod 4$, hence the following Corollary.

Corollary 15 *If $N = 2n'$, for some integer n', then Hermitian self-dual negacyclic codes over $\mathbb{F}_{q^2}$ of length n exist if and only if*

$$q \equiv 1 \mod 4.$$

Theorem 16 *Let $n = 2^a n'$, $a > 1$ and $q \equiv 1 \mod 2^a n''$, such that $n'|n''$ and n'' odd. Then there exists an MDS negacyclic codes which is Hermitian self-dual with defining set*

$$T = \{i \ odd : 1 \leq i \leq n-1\}.$$

Proof. If $q \equiv 1 \mod 2^a n''$, then $q \neq -1 \mod 2^{a+1}$. Because if it is the case, then $q = -1 + k2^{a+1}$ and $q = 1 + 2^a n'' k'$, by summing the two quantities of q and dividing by 2 both sides, we have $q = 2^{a-1}(n''k' + 2k)$. This implies that q is even, since $a > 1$, which is impossible. Hence by Proposition 14 we have $C_{q^2}(-qi) \neq \{i\}$, since we proved that $q \neq -1 + k2^{a+1}$. For these parameters we have $\xi \in \mathbb{F}_{q^2}$. Then by a similar argument as Theorem 12 we have that

n	q	n	q	n	q
12	13,5^2,37,7^2,97	20	41,61,81,101,181	24	5^2,7^2,73,97,121
28	29,113,197	36	37,73,109	40	41,9^2,11^2
42	43,127	48	7^2,97	60	61,181
44	89,353	48	97,193,241,281,337	52	53,157,313,

TABLE 5 – Hermitian Self-dual MDS Codes over $\mathbb{F}_{q^2}$ obtained by Theorem 16

$C_{q^2}(i) = \{i\}$. Now, we prove that for $i, j \in T$ we cannot have $C_{q^2}(-qi) = \{j\}$. Assume it is the case, then we will have $2kn - qi = j$. The last equality is equivalent to $2^{a+1}n'k - 2^a n''k' = i + j \iff 2^a(2k - \frac{n''k'}{n'}) = i + j$. Hence $2^a n'$ divides $i + j$. But i and j odd gives $i + j = 2(1 + 2k'')$. This gives a contradiction since we assumed $a > 1$. Hence by Lemma 13 we obtain $T^{\perp h} = T$. Hence the code is Hermitian self-dual. By the BCH bound the minimum distance is $n/2 + 1$. ■

A generalization of the splitting of n to the negacyclic codes whose introduced in [3].

A q splitting of n is a multiplier μ_s of n that induce a partition of O_{2n}, such that

1. $O_{2n} = A_1 \cup A_2 \cup X$
2. S_1, S_2 and X are unions of q cyclotomic classes.
3. $\mu'_s(S_i) = S_{i+1(\mod 2)}$ and $\mu'_s(X) = X$.

A q splitting is of type I, if $X = \emptyset$. A q splitting is of type II if $X = \{\frac{n}{2}, \frac{3n}{2}\}$.

Definition 17 *A negacyclic code C of length n over $\mathbb{F}_q$ is duadic if there* *exists a such splitting and the defining set is one of the subset S_i or $S_i \cup X$. If the splitting is of type II, then there exists polynomials $A_i(x)$ such that $x^n + 1 = A_1(x)A_2(x)(x^2 + 1)$ and $\mu_s(A_i(x)) = A_{i+1}(x)$.*

Remark 18 *An Euclidean respectively Hermitian self-dual negacyclic code is duadic with multiplier μ_{-1} respectively μ_{-q} and comes from type I splitting.*

In the next we consider negacyclic code with length $n = 2p^t$, with p an odd prime.

Lemma 19 *([3, Theorem 8]) If p, q are distinct odd primes, $q \equiv 3 \mod 4$ and $r = \operatorname{ord}_{2p^t}$ is the order of q modulo $2p^t$, then we have the following which holds.*

1. *There exists a q splitting of $n = 2p^t$ of type II.*
2. *μ_{-1} gives a splitting of n of type II if and only if $r \neq 2 \mod 4$.*

Remark 20 *We have $r = \operatorname{ord}_{2p^t} q = lcm(\operatorname{ord}_2 q, \operatorname{ord}_{p^t} q) = \operatorname{ord}_{p^t} q$, since q is odd. Let z be the largest integer such that $p^z|(q^t - 1)$, with t order of q modulo p. Hence if $z = 1$, we have $\operatorname{ord}_{p^t} q = p^{t-1} \operatorname{ord}_p q$ [8, Lemma 3.5.4]. Hence if $\operatorname{ord}_p q$ is odd or $\operatorname{ord}_p q \equiv 0 \mod 4$, then $r \neq 2 \mod 4$. Hence from Lemma 19 the multiplier μ_{-1} gives a splitting of n of type II.*

Lemma 21 *Let p and q be odd prime number, hence we have the following.*

1. *If $p \equiv 1 \mod 4$ and $(\frac{q}{p}) = -1$, hence $\operatorname{ord}_p q \equiv 0 \mod 4$.*
2. *If $(\frac{q}{p}) = 1$ and $p \equiv 3 \mod 4$, hence $\operatorname{ord}_p q$ is odd.*

Proof. If we assume that q is not a quadratic residue modulo p. Hence from [14, Lemma 6.2.2] $\operatorname{ord}_p q$ is not a divisor of $\frac{p-1}{2}$. Then from Fermat's Theorem $\operatorname{ord}_p q = p-1$, hence $\operatorname{ord}_p q \equiv 0 \mod 4$, since $p \equiv 1 \mod 4$.

If $q = \square \mod p$, hence from [14, Lemma 6.2.2] $\operatorname{ord}_p q$ is a divisor of $\frac{p-1}{2}$. Since, $p \equiv 3 \mod 4$, then $\frac{p-1}{2}$ odd which implies $\operatorname{ord}_p q$ is also odd. ■

Assume, that the following equation

$$2 + \gamma^2 n = 0 \tag{9}$$

has a solution in $\mathbb{F}_q$. If $\mathsf{a} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, define

$$\widetilde{\mathsf{a}} = (a_0, \ldots, a_{n-1}, a_\infty, a_*) \in \mathbb{F}_q^{n+1},$$

where

$$a_\infty = \gamma \sum_{i=0}^{\frac{n-1}{2}} (-1)^i a_{2i}, \;\; a_* = \gamma \sum_{i=0}^{\frac{n-1}{2}} (-1)^i a_{2i+1}.$$

The set $\widetilde{C} = \{\widetilde{\mathsf{a}} = (a_0, \ldots, a_{n-1}, a_\infty, a_*) \in \mathbb{F}_q^{n+1} : (a_0, \ldots, a_{n-1}) \in C\}$ is a linear code of $\mathbb{F}_q$.

Lemma 22 *([3, Theorem 12])*

Let q be a prime power and γ is a solution of the equation (9) in $\mathbb{F}_q$, and suppose that D_1 and D_2 are odd-like negacyclic duadic codes of length $n = 2p^t$, with multiplier μ_{-1} of type II. Then $\widetilde{D_i}$ for $i = 1, 2$ are self-dual.

Lemma 23 *Let q, p be odd prime such that $q \equiv p \equiv 3 \mod 4$, $n = 2p^t$, with*

t odd. Hence the equation (9) has a solution in $\mathbb{F}_q$

Proof. There is a solution for the equation $2 + 2p\gamma^2 = 0$ in $\mathbb{F}_q$ if and only if there is a solution of $1 + p\gamma^2 = 0$ in $\mathbb{F}_q$. If we assume $p \equiv 3 \mod 4$, the last equation has a solution $\gamma \in \mathbb{F}_q$ from [14, Lemma 6.6.17]. If t is odd γ^t is a solution of the equation (9). ■

Theorem 24 *Let p, q, be two odd primes such that $q = \Box \mod p$, $q \equiv p \equiv 3 \mod 4$ and $z = 1$. Then there exists negacyclic duadic codes of length $n = 2p^t$, t odd, with splitting of type II given by μ_{-1}, and such that $\widetilde{D_i}$ are self-dual for $i = 1$ and 2.*

Proof. If we have such p and q from Lemma 21 the $\mathrm{ord}_{2p^t} q$ is odd. Hence from Remark 20 μ_{-1} gives a splitting of n of type II. Furthermore, from Lemma 23 the equation (9) has a solution in $\mathbb{F}_q$. Hence from Lemma 22 The codes D_i are extended to self-dual codes $\widetilde{D_i}$, for $i = 1$ and 2. ■

If we assume $q \equiv 3 \mod 4$, $p \equiv 1 \mod 4$, $z = 1$ and q not residue quadratic modulo p, hence from Lemma 21 the $\mathrm{ord}_{2p^t} q \equiv 0 \mod 4$. Hence from Remark 20 μ_{-1} gives a splitting of n of type II. Hence there exist duadic negacyclic codes. Unfortunately in this case we cannot extend the codes in order to get self-dual codes as we done in Theorem 24. That is because simply the equation (9) has no solution in $\mathbb{F}_q$. Namely, a solution will implies that $(\frac{-p^t}{q}) = 1$. But, we have $(\frac{-p^t}{q}) = (\frac{-1}{q})(\frac{p^t}{q})$. Since $q \equiv 3 \mod 4$, hence -1 is not a quadratic residue modulo q. Then $(\frac{-p^t}{q}) = -(\frac{p^t}{q})$. Furthermore, from the law of quadratic reciprocity, we have $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1$. As

p	Arguments
109	Theorem 12
137	Theorem 7
181	Theorem 12
197	Theorem 11
233	Theorem 11
269	Theorem 11

Table 6 – MDS self-dual $[18, 9, 10]$ over $\mathbb{F}_p$

$(\frac{q}{p}) = -1$, this implies $(\frac{p}{q}) = 1$. Hence $(\frac{p^t}{q}) = 1$.

Gulliver and Harada [10] proved the existence of MDS self-dual codes of length 18 over $\mathbb{F}_p$, whenever $17 \leq 97$. But when $101 \leq p \leq 300$ they gave quasi-twisted self-dual $[18, 9, 9]_p$ from unimoduallar lattices [10, Table 3]. In the following table we give some examples of MDS self-dual codes of length 18, for $p \geq 101$.

Acknowledgment

The author would like to thank Professor Thierry P. Berger for help and encouragement in carrying out the research in this paper.

Références

[1] E. F. Assmus, H. F. Mattson, Jr., *New five designs*, J. Comb. Theory. (6), 122-151, 1969.

[2] N. Aydin, I. Siap and D. J. Ray-Chaudhuri, *The structure of 1-generator quasi-twisted codes and new linear codes*, Des. Codes Cryptogr. 24(3), 313-326, 2001.

[3] T. Blackford, *Negacyclic duadic codes*, Finite Fields Appl. 14, 930-943, 2008.

[4] K. Betsumiya, S. Georgiou, T. A. Gulliver, M. Harada and C. Koukouvinos, *On self-dual codes over some prime fields,* Disc. Math, 262, 37-58, Feb. 2003.

[5] L. Dicuangco, P. Moree and P. Solé, *The lengths of Hermitian self-dual codes,* J. Pure Appl. Algebra, 209, 1, Ap. 2007.

[6] S. R. Ghorpade and G. Lachaud, *Hyperplane Section of Grassmannians and the number of MDS Linear Codes Finite field and their applications,* Academic press, 7 (4), 468-506, Oct. 2001.

[7] K. Guenda, *Quantum Duadic and Affine Invariant Codes.* Internat. J. Quantum Information, 2(1) : 757-775, Feb. 2009.

[8] K. Guenda, *Sur l'équivalence des Codes,* Ph.D. thesis University of Science and Technology, U.S.T.H.B, Algiers, Algeria.

[9] T. A. Gulliver, J. L. Kim and Y. Lee *New MDS or near MDS self-dual codes,* IEEE. Trans. Inform. Theory, 54, 4354-4360, 2008.

[10] T. A. Gulliver, M. Harada *MDS self-dual codes of lengths 16 and 18 MDS or near MDS self-dual codes,* Int. J. Inform. Coding Theory, xx, xxx-xx, 2010.

[11] Hai Quang Dinh, Lopez-Permount, *Cyclic and negacyclic codes over finite chain rings,* IEEE. Trans. Inform. Theory, 36(4), 1728-1744, 2004.

[12] R. Hill, *An extension theorem for linear codes,* Designs, Codes and Cryptography, 17, 151-157, 1999.

[13] W. C. Huffman, V. Job and V. Pless, *Multipliers and generalized multipliers of cyclic objects and cyclic codes.* J. Comb. Theory A(62) 1993.

[14] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes,* Cambridge, 2003.

[15] J. L. Kim and Y. Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields* J. Combin. Theory A, 105, 79-95, 2004.

[16] I. A. Kotsireas, C. Koukouvinos and D. Simos, *MDS and near-MDS self-dual codes over large prime fields,* Advan. Math Comm. 3, 4, 349-361, 2009.

[17] A. Krishna and D. V. Sarwate, *Pseudo-cyclic MDS codes,* IEE Trans. Inform. Theory, 36(4), Jul. 1990.

[18] J. M. Jensen, *Cyclic concatenated codes with constacyclic outer codes,* IEEE Trans. Inform. Theory, 38(3), 950-959, 1992.

[19] F.J. Macwilliams and N.J.A Sloane, *The theory of error correcting-codes,* Benjamin, Inc. Amsterdam, North-Holland, 1977.

[20] P. Pedersen C. Dahl, *Classification of pseudo-cyclic MDS codes,* IEEE Trans. Inform. Theory, 37(2), Mar. 1991.

[21] V. Pless and J. N. Pierce, *Self-dual codes over $GF(q)$ satisfy a modified Varshamov-Gilbert bound,* Inform. and control, 23, 35-40, 1973.

[22] S. Roman, *Coding and information theory,* Springer Verlag, New-York, 1992.

[23] M. H. M. Smid, *Duadic codes,* IEEE. Trans. Inform. Theory, 29(2), 1983.